March 21, 2003

Information System Security

Controls Over the Use and Protection of Social Security Numbers Within DoD
(D-2003-066)

Department of Defense
Office of the Inspector General

Quality *Integrity* *Accountability*

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
21 Mar 2003	N/A	-

Title and Subtitle Information System Security: Controls Over the Use and Protection of Social Security Numbers Within DoD	**Contract Number**
	Grant Number
	Program Element Number
Author(s)	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) OAIG-AUD(ATTN: AFTS Audit Suggestions) Inspector General Department of Defense 400 Army Navy Drive (Room 801) Arlington, VA 22202-2884	**Performing Organization Report Number**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	
Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** UU
Number of Pages 26	

Additional Copies

To obtain additional copies of this audit report, contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, DC 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

AAFES	Army and Air Force Exchange Service
DMDC	Defense Manpower Data Center
DSS	Defense Security Service
FAR	Federal Acquisition Regulation
GAO	General Accounting Office
SSN	Social Security Number

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

March 21, 2003

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS
ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGENCE)
ASSISTANT SECRETARY OF THE AIR FORCE (FINANCIAL MANAGEMENT AND COMPTROLLER)
DIRECTOR, ARMY AND AIR FORCE EXCHANGE SERVICE
DIRECTOR, DEFENSE SECURITY SERVICE

SUBJECT: Report on Controls Over the Use and Protection of Social Security Numbers within DoD (Report No. D-2003-066)

We are providing this report for information and use. This report is in response to a request by the General Accounting Office for member Inspectors General of the President's Council on Integrity and Efficiency to review the use of Social Security Numbers within their agencies. We considered management comments on the draft of this report when preparing the final report.

Comments conformed to the requirements of DoD Directive 7650.3; therefore, additional comments are not required. However, since management at the three DoD organizations reviewed agreed to take various corrective actions, we ask that these organizations provide proposed or actual completion dates for these actions. This will facilitate follow-up actions. See Page 10 for specific corrective actions.

We appreciate the courtesies extended to the staff. Questions should be directed to Mr. Bruce A. Burton at (703) 604-9071 (DSN 664-9071) or Mr. Thomas S. Bartoszek at (703) 604-9014 (DSN 664-9014). See Appendix B for the report distribution. The team members are listed inside the back cover.

Thomas F. Gimble

David K. Steensma
Deputy Assistant Inspector General
for Auditing

Office of the Inspector General of the Department of Defense

Report No. D-2003-066 **March 21, 2003**
(Project No. D2002AB-0070)

Controls Over the Use and Protection of Social Security Numbers Within DoD

Executive Summary

Who Should Read This Report and Why? Program administrators, developers, managers, and users of systems of records, and all DoD personnel interested in how DoD uses and protects Social Security Numbers.

Background. This report is in response to a request by the General Accounting Office for member Inspectors General of the President's Council on Integrity and Efficiency to conduct a review on the use of Social Security Numbers within their agencies and to verify the information reported on a General Accounting Office questionnaire. The four DoD agencies that responded to the General Accounting Office questionnaire were the Defense Manpower Data Center, the Army and Air Force Exchange Service, the Defense Security Service, and the Tricare Management Activity.

While this report addresses the use of Social Security Numbers within DoD and verifies information reported on a General Accounting Office questionnaire, other reviews by the Office of the Inspector General, Department of Defense, focused on the adequacy of controls over contracting including use of the Privacy Act clauses in contracts and the disposal of personally identifiable information.

In 1967, DoD adopted the Social Security Number instead of the Military Service Number for identifying Armed Forces personnel. The Social Security Number has become the most widely used identifier in both public and private sectors.

The Privacy Act of 1974 (Public Law 93-579) states the right to privacy is a personal and fundamental right protected by the Constitution of the United States. The Privacy Act states that the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies.

Social Security Numbers are used for employee files, medical records, health insurance accounts, credit and banking accounts, university identification cards, and many other purposes, and we believe that there is a higher risk of misuse and potential for identity theft resulting in monetary losses to individuals and businesses.

Results. We reviewed three of the four DoD agencies that responded to the General Accounting Office questionnaire. Those three agencies made disclosures of personally identifiable information for legal purposes; however, their Privacy Programs needed improvements in policy administration, oversight, periodic reviews, physical security, and training.

After we notified officials at the DoD agencies of our findings, they concurred and took or agreed to take the necessary remedial actions to mitigate the risk of improper disclosure of Social Security Numbers. Those actions will help the agencies improve appropriate controls over contractors' and other entities' access to and use of the Social Security Numbers maintained in their databases.

Management Comments. We provided a draft of this report to those DoD agencies on November 12, 2002. Written responses to this report were obtained before we issued the draft report. Those comments are included in the Management Comments section.

While we made no recommendations because the three DoD organizations agreed to take appropriate corrective actions, we ask that the Defense Manpower Data Center, the Army and Air Force Exchange Service, and the Defense Security Service provide planned or completed dates for agreed-upon actions. The specific agreed-upon corrective actions are included on page 10 of the report.

Table of Contents

Background

Social Security Numbers. The Social Security Number (SSN) was created in 1936 to track workers' earnings for calculating Social Security retirement benefits. When SSNs were first introduced, the Federal Government assured the public that use of the numbers would be limited to Social Security programs. However, the SSN has become the most widely used identifier in the public and private sectors. Because SSNs are used for employee files, medical records, health insurance accounts, credit and banking accounts, university identification cards, and many other purposes, there is potential for identity theft resulting in monetary losses to individuals and businesses. In 1967, DoD adopted the SSN instead of the Military Service Number for identifying Armed Forces personnel.

Privacy Act of 1974. The Privacy Act of 1974 (Public Law 93-579) states the right to privacy is a personal and fundamental right protected by the Constitution of the United States. The Privacy Act states that the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies. The increasing use of computers and sophisticated information technology has increased the threat to individual privacy that can occur when collecting, maintaining, using, and disseminating personal information. The purpose of the Privacy Act is to provide certain safeguards for an individual against the invasion of privacy. One of the purposes of the Privacy Act is to permit individuals to determine which records pertaining to them are collected, maintained, or disseminated to other agencies. DoD Policy prohibits disclosure of personally identifiable records maintained by Government agencies without a person's consent, and grants individuals the right to access and amend those records if they are not accurate, relevant, current, or complete.

DoD Directive 5400.11,"DoD Privacy Program, " December 13, 1999. The Directive states that personal information such as SSNs that identifies individuals shall be collected, maintained, used, and disclosed only when it is relevant and necessary to accomplish a lawful DoD purpose. When collected, the agency must inform the individual why the information is being collected, the authority for collection, whether the disclosure is mandatory or voluntary, and the consequences of not providing that information. The Directive permits individuals to determine to the extent authorized by the Privacy Act, which records pertaining to them are contained in a system of records maintained by a DoD Component. It permits an individual to gain access to such records that pertain to them, obtain a copy of the records, correct inaccurate information on a showing that the records are not accurate, relevant, current, and complete, and appeal a denial of access or a request for amendment to those records. The Directive defines a record as any collection of information about an individual that identifies, relates to, or is unique to an individual, such as a SSN. A group of records is called a system of records. Before a system of records is established and personally identifying information is obtained, a notice of the system of records must first be published in the Federal Register. Publication in the register constitutes official public notice. The Directive also states that once the information is collected, appropriate safeguards will be established to ensure the security of the records. Components must issue procedures, conduct periodic reviews, and train personnel on their Privacy Program.

Federal Acquisition Regulation. The Federal Acquisition Regulation **(**FAR) Part 24, " Protection of Privacy and Freedom of Information," prescribes policies and procedures that apply the requirements of the Privacy Act of 1974 to Government contracts. The FAR requires contracting officers to insert Privacy Act clauses 52.224-1 and 52.224-2 in contracts. When the design, development, or operation of a system of records on individuals is required to accomplish an agency function, the clauses require contractors to comply with the Privacy Act of 1974.

General Accounting Office Review. The House Ways and Means Committee, Subcommittee on Social Security and the Senate Judiciary Committee, Subcommittee on Technology, Terrorism, and Government Information requested the General Accounting Office (GAO) to review the Government's use of SSNs. The review began in March 2001 and examined the Federal, State, and local governments' use of SSNs to administer programs, provide services to the public, protect individuals' privacy, and prevent identity theft**.** The review focused on 18 Federal agencies including DoD. GAO sent a questionnaire to the agencies on their use and protection of SSNs. The GAO review formed the basis for the President's Council on Integrity and Efficiency's request for member Inspectors General to review the use of SSNs in their agencies, verify the information provided to GAO and report the findings to the Social Security Administration, Office of the Inspector General.

DoD Organizations Reviewed. The GAO sent the questionnaire to four DoD agencies. We reviewed information for the Defense Manpower Data Center (DMDC), the Army and Air Force Exchange Service (AAFES), and the Defense Security Service (DSS).

DMDC. The DMDC reports to the Under Secretary of Defense for Personnel and Readiness. DMDC is the central repository of all DoD human resource information. Its mission is to collect, provide, and use the central repository of information for the benefit of DoD decision makers, DoD organizations, and other Government agencies. In 2001, DMDC received and archived more than 5,000 separate databases containing more than 1.25 billion individual records.

AAFES. The AAFES is a military organization that provides quality retail merchandise and services at low prices to members of the Armed Forces, military retirees, and their families. The AAFES returns its earnings to the Army and Air Force to improve the quality of life for military families. Although AAFES is a Federal organization, it is a nonappropiated fund instrumentality that does not rely on appropriated tax dollars for major support. The AAFES operates almost exclusively with funds generated from its business income.

DSS. The DSS is a security organization providing personnel investigations, industrial security products and services, and comprehensive security training to DoD and other Government agencies. DSS investigative agents conduct personnel security investigations of military personnel, DoD civilians, Defense contractors, and other authorized personnel. DSS also provides oversight and assistance to Defense contractors.

Objectives

The objective was to determine whether DoD agencies maintain appropriate controls over the access, disclosure, and use of SSN information by third parties. Specifically, we determined whether the selected DoD agencies made disclosures of SSNs to third parties for legal purposes, whether selected DoD agencies had appropriate controls over the contractors' and other entities' access and use of SSNs, and whether the selected agencies had adequate controls over access to individuals' SSNs maintained in their databases. In addition, we verified the information on the questionnaires completed for the GAO. See Appendix A for a discussion of the scope and methodology and prior audit coverage.

Use and Protection of Social Security Numbers in DoD

Although the three DoD agencies made disclosures of personally identifiable information for legal purposes to third parties, improvements in the Privacy Program were needed in contract administration, policy, periodic reviews, physical security, and training. Additional safeguards were required because:

- procedures were incomplete,
- oversight and administration of contracts was inadequate,
- periodic reviews of the Privacy Program were not conducted,
- physical security measures for information systems that store social security numbers were poor, and;
- privacy act training was not provided.

As a result, we believe the three DoD agencies had increased risk for SSN misuse and identity theft that could result in potential monetary loss to individuals and businesses. After the agencies were notified of the issues, they initiated corrective actions.

Disclosures of SSNs

The three DoD agencies we reviewed made disclosures of personally identifiable information for legal purposes. DoD Directive 5400.11 states that personal information that identifies individuals shall be collected, maintained, used, and disclosed only when it is necessary to accomplish a lawful DoD purpose. The agency must inform the individual why the information is being collected and publish a notice for all systems of records.

DMDC. The DMDC is the central repository of all DoD human resource information. We reviewed two systems that were the focus of the GAO review, including the Military Entrance Processing Command File and the High School Students Armed Services Vocational Aptitude Battery File. DMDC did not collect the data for both systems, but was the custodian of the information obtained. DMDC provided the information in those files to other DoD decision makers, DoD organizations, and other Government agencies. DMDC has memorandums of understanding with entities to whom they release information. All entities are required to release the information only to authorized officials. In addition, DMDC has 10 systems of records. We reviewed the largest system which provides a single central facility within DoD to assess manpower trends, support personnel and readiness functions, perform statistical analyses, assist in detecting fraud and abuse of pay and benefits and register former and current

DoD civilian and military personnel for the purpose of determining medical and other benefits. The notice for this system of records was published in the Federal Register.

AAFES. Employees and customers of AAFES are adequately informed about the collection, disclosure, and use of their SSNs. Officials stated AAFES provides SSNs to Government agencies and AAFES contractors for employee and customer benefits and services including health coverage, retirement benefits, payroll taxes, check cashing privileges, and exchange credit cards. AAFES has 27 official systems of records used to accomplish AAFES functions. We reviewed 23 of these systems. Notices for the systems of records were published in the Federal Register.

DSS. DSS discloses information identifying individuals' SSNs to non-Government and Government entities. When personal information is collected, individuals are informed of the intended use and disclosure. DSS discloses personal information to law enforcement offices, such as local and state police departments and credit bureaus. DSS maintains 15 official systems of records. We reviewed three of those systems because they were the focus of the DSS primary mission of security investigations. Those records were recorded in notices and published in the Federal Register. We also reviewed the process used by DSS to protect privacy data during the conduct of personnel security investigations. DSS has an accreditation process with its customers to ensure that personally identifiable information provided to others is properly identified, obtained, used, and disposed.

Procedures on the Privacy Program

Of the three agencies reviewed, two did not have complete procedures to address the Privacy Program. DoD Directive 5400.11 requires that procedures be issued addressing the Privacy Program.

DMDC. DMDC published the "Personnel Data Release and Acquisition Policy," April 25, 2001, which addresses the release of Privacy Act information and provides legal accountability for all data released from DMDC that is individually identifiable. However, the policy did not define a process to release data to other DoD organizations, Government organizations, and others. Officials agreed to revise the policy to include the process to be followed when releasing personally identifiable data. The revised policy would ensure consistent practices on requests to obtain personally identifiable information such as SSNs and the release of the data. Because officials agreed to take action, we did not make a recommendation.

AAFES. The AAFES established procedures to implement the DoD Privacy Program requirements. The AAFES Exchange Operating Procedures 11-1 "AAFES Privacy Program," dated July 16, 2001, provides adequate policies, procedures, a process, and guidance for its Privacy Program.

DSS. DSS established procedures to implement the DoD Privacy Program requirements. DSS Regulation 01-13-R "Privacy Program," dated

January 2, 2001, and DSS Regulation 20-12 " Investigation – Protection and Release of Investigative Information," dated June 30, 2000, provide rules, policies and procedures for the disclosure of personal records in the custody of DSS. However, DSS did not have an overarching standard operating procedure that detailed its personnel security investigations process from beginning to end. DSS officials acknowledge that the standard operating procedures manual was last printed in 1993. The manual describes the DSS Personnel Investigation Center mission, operational policies, and procedures. Officials stated that although a new process had been implemented and procedures for opening, monitoring, and closing cases had changed, the basic structure and mission had not. In addition, DSS provided a handbook and a manual to employees that provide direction, guidance, and standards for investigations and Privacy Act protection and disclosure. While all of those measures help, officials agreed that an updated standard operating procedure was needed to increase the consistency of how data is protected and processed. Officials are obtaining contractual support for the development and publication of up-to-date operating procedures. The planned policy revision will ensure that information requested by other organizations will be reviewed for approval, documented, and submitted in accordance with the DoD Directive and the Privacy Act. Accordingly, we did not make a recommendation.

Contract Administration and Oversight

Two of the three agencies reviewed did not ensure that all contracts included the appropriate FAR clauses requiring contractors to adhere to the requirements of the Privacy Act. In addition, officials did not monitor contractors to ensure that they protected system of records information. The FAR requires contracting officers to insert Privacy Act clauses 52.224-1 and 52.224-2 in contracts that pertain to the collection of personally identifiable information.

DMDC. DMDC employs contractors to help it meet its mission to collect, provide, and use the central repository to provide information to DoD decision makers, DoD organizations, and other Government agencies. According to a DMDC official, DMDC uses a General Services Administration supply-and-service contract that includes the Privacy Act clauses. The contract provides for services at a fixed price. DMDC places an order against the General Services Administration contract for the services. While we did not review the contract, DMDC officials stated that the contract contained the appropriate Privacy Act clauses. Officials at the General Services Administration stated that they do not verify compliance with the Privacy Act clause because it is the responsibility of the organization who places an order against the General Services Administration contract. We believe that risk of compromise of privacy data is lower because contractor personnel are located at DMDC, which is a secured site. In addition, DMDC personnel monitor and restrict the access of contractor personnel to only appropriate data required to perform their duties.

AAFES. Officials stated AAFES provides SSNs to contractors to process health care benefits, retirement benefits, disability benefits, employment applications, background investigations, unemployment claims, employment verifications, employee assistance services, credit bureau reporting, and bad check and debt

collections. AAFES is a nonappropriated fund instrumentality and therefore is not required to follow the FAR. However, provisions of the Privacy Act should still be applied to a nonappropriated fund instrumentality. Of the 21 contracts at AAFES we reviewed, 16 included requirements for data protection. However, only 5 of the 16 included the Privacy Act clauses. There was no uniformity in language or requirements relating to the protection of personal information. In addition, AAFES officials stated they did not monitor contractor performance relating to the Privacy Act. AAFES officials agreed to use uniform Privacy Act statements or confidentiality provisions that the information will be used only for the purpose provided. Accordingly, we did not make a recommendation.

DSS. DSS officials stated DSS has contracts with 12 firms. The firms provide background investigations and credit histories on DoD personnel, and maintain a computer operations center. Only 1 of the 12 contracts we reviewed contained the required Privacy Act FAR clauses. In addition, DSS did not adequately review and monitor how contractors used and disposed of data containing SSNs. For example, one contractor was improperly disposing of personnel background sheets that contained individuals' SSNs and a credit bureau was using DSS data to update its database files. While the contract with the credit bureau did not prohibit an update to its files, an official from the DoD Privacy Office stated that the contract should have contained the confidentiality clause and this omission resulted in a violation of the Privacy Act. General Counsel at DSS informed us that the credit bureau had reviewed its database and eliminated information it obtained as a result of the contract with DSS. He stated that it was unnecessary for the credit bureau to again review their database because the update had occurred a long time ago and there have been no new complaints. Other reviews by the Office of the Inspector General, Department of Defense, focused on the adequacy of controls over contracting including use of the Privacy Act clauses in contracts and the disposal of personally identifiable information at the Defense Security Service.

We provided our findings to DSS officials who agreed to take necessary action to remedy the deficiencies. They agreed to modify each contract to include the appropriate FAR clauses, conduct unannounced visits at contractor sites, and conduct routine data protection reviews. They also agreed to assign a contracting officer representative to contact each credit bureau to ensure that changes to individual records were not made from information that DSS supplied. Accordingly, we did not make a recommendation.

Privacy Act Program Review

All three DoD agencies reviewed were not conducting periodic reviews of the Privacy Program. DoD Directive 5400.11 requires periodic reviews of the Privacy Program by the agency's Inspector General or other officials who have specialized knowledge of the DoD Privacy Program.

DMDC. Officials at DMDC stated that periodic reviews of the Privacy Program were not conducted because it lacked personnel to perform this duty. However, as a result of our visit, DMDC officials agreed to start performing reviews. Accordingly, we did not make a recommendation.

AAFES. Officials at AAFES stated that they performed periodic reviews of the Privacy Program until 1999. However, when Congress eliminated the reporting requirement on the number of access and amended requests processed, AAFES officials stated they ceased performing the reviews. As a result of our visit, AAFES officials agreed to periodically perform internal audits addressing Privacy Act oversight and verification of SSN use and protection. Accordingly, we did not make a recommendation.

DSS. Officials at DSS stated that they performed the last review of the Privacy Program in 1994. By 1997, the Director and senior staff of DSS stopped the Inspector General inspection process and changed the Inspector General office to Strategic Planning. In 1999, the Inspector General office was reestablished and the inspection process resumed. The Office of the Inspector General for the Defense Security Service scheduled an inspection of the Office of Freedom of Information and Privacy from September 9 through September 12, 2002. The Privacy Act Office inspection was completed on September 20, 2002. While there was a long delay in the review of the program, the reestablishment of the Inspector General office and the September inspection are positive steps. As a result, we did not make a recommendation.

Physical Security of Information Systems

One of the three DoD agencies reviewed did not secure information systems that contained SSNs. DoD Directive 5400.11 requires that privacy information be secured.

DMDC. The DMDC mainframe computer is located off-site. At certain times during the week, the mainframe is in an area that is not staffed and has minimal physical security. Although the system of records that contains SSNs could not be accessed or manipulated without the use of special equipment, the area that housed the mainframe stored components that contained personally identifiable information. Officials at DMDC agreed to consult a security professional to perform a risk assessment of the vulnerability of the mainframe and storage media. Therefore, we did not make a recommendation.

AAFES. The AAFES has safeguards to ensure the protection of sensitive information including Privacy Act data. The buildings have guards, and badges and escorts are required. The data center where the mainframes are located is monitored 24 hours a day, 7 days a week, with access controlled by badges and personnel identification numbers. Officials stated that computer safeguards include user identification, password protection, firewalls, and intrusion detection systems. Officials stated that third-party access to the AAFES intranet is limited, because most data is retrieved from the systems of records into data sets and then provided securely to outside entities.

DSS. DSS has safeguards to ensure the protection of systems that maintain sensitive information, including SSNs. Access at all DSS locations is restricted to authorized personnel with proper identification. The buildings have guards posted at the entryways, who check badges. Escorts are provided, when needed. Additionally, the Personnel Investigation Center, where personnel security

investigations data are maintained, is located on a secure military base. There are cipher locks in the area where the computer terminals are located. All users of DSS information systems must obtain security clearances. Officials stated that computer safeguards include user identification, password protection, encrypted data transmission, and transportation of hard copies through approved sources. In addition, the computer system records user access.

Privacy Act Training

One of the three DoD agencies reviewed did not provide employees with the required Privacy Act training. DoD Directive 5400.11 requires Components to hold training sessions on their Privacy Programs.

DMDC. Privacy Act training is required for new employees and other staff on a yearly basis. Employee training lasts for 1 hour and covers the Privacy Act and Freedom of Information Act**.** New employee training addresses the mission of the organization, job descriptions, organization charts, the Privacy Act, and the Freedom of Information Act.

AAFES. AAFES employees who work with the Treasury Offset Program are required to read the Treasury Offset Program pamphlet and view a video on protection of taxpayer information annually. This is an Internal Revenue Service requirement and AAFES must annually provide a Safeguard Activity Report on how AAFES protects taxpayer data. However, AAFES officials stated they had no employee training on the DoD Privacy Program, Privacy Act requirements, and the protection and use of SSNs. Officials at AAFES stated that they overlooked the requirement; however, they would produce a video for distribution to AAFES facilities worldwide concerning the Privacy Act and the use and protection of SSNs. Accordingly, we did not make a recommendation.

DSS. DSS established a training curriculum to inform employees how to safeguard information covering the Freedom of Information Act and the Privacy Act. The DSS provides an annual security refresher briefing. The DSS Security Division provides the training that outlines the objectives of the Privacy Act, and the agencies' responsibilities for maintaining, requesting, and disclosing Privacy Act information. In addition, DSS requires its contractors who conduct personnel security investigations to conduct and receive periodic training in handling and processing confidential and Privacy Act data. According to DSS, future DSS contracts will stress Privacy Act training and data protection.

Summary

The Privacy Act of 1974 states the right to privacy is a personal and fundamental right protected by the Constitution of the United States. The Privacy Act provides that the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal Agencies. The increasing use of computers has increased the potential for harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information. Agencies need to make informed

disclosures for legal purposes when collecting and releasing personally identifiable information such as SSNs. The procedures in the Privacy Program define the rules of the agency and the process to carry out the mission as it relates to the Privacy Program. The contract administration and oversight function allows agencies to oversee the functions of its contractors, who must follow the same general rules as the agency. The physical security of information protects the systems from misuse, and training keeps employees informed on the requirements of DoD Directives and the Privacy Act. All improvements will reduce the risk of unauthorized loss of control over personally identifiable data entrusted to DoD and its contractors.

Planned Actions by Management

DMDC. The following actions were agreed to by DMDC:

1. Revise Privacy Policy to include the process to be followed when releasing personally identifiable data,
2. Start performing reviews of the Privacy Program, and
3. Consult a security professional to perform a risk assessment of mainframe and storage media vulnerability.

AAFES. The following actions were agreed to by AAFES:

1. Use uniform Privacy Act statements or confidentiality provisions and include those provisions in all contracts,
2. Conduct periodic reviews of the Privacy Program, and
3. Produce a video on the Privacy Act and use and protection of SSNs and distribute the video to its facilities worldwide.

DSS. The following actions were agreed to by DSS:

1. Update standard operating procedures for protection and release of privacy data,
2. Modify contracts to include appropriate FAR clauses,
3. Conduct unannounced visits to contractor sites, and
4. Assign a representative to ensure that credit bureaus did not make changes to individual credit records from data provided by DSS for other purposes.

Appendix A. Scope and Methodology

We visited the Defense Manpower Data Center, the Army and Air Force Exchange Service, and the Defense Security Service. We reviewed 38 systems of records, 33 contracts, and 10 facilities. We reviewed the agencies' controls over the use, disclosure, and access to SSN information by third parties, interviewed agency officials responsible for controlling SSN disclosure and access, verified and updated key pieces of information provided on GAO questionnaires, and provided examples of additional steps that the agencies can take to ensure that it has adequate controls over the use and protection of SSNs. We also reviewed four contractors and their controls over the use, disclosure, and access to SSN information. We did not review the controls over contracting at the Defense Manpower Data Center, the Army and Air Force Exchange Service, and the Defense Security Service. The controls over contracting at Defense Security Service is being reviewed under a separate audit by the Inspector General, Department of Defense. We also did not test the software application used to monitor and control access to the data files that contained personally identifiable information.

We performed this audit from January 2002 through October 2002 in accordance with generally accepted government auditing standards. The management control program was not an announced objective and was not reviewed due to time constraints**.**

Use of Computer-Processed Data. We did not use computer-processed data to perform this audit.

General Accounting Office High-Risk Area. The General Accounting Office has identified several high-risk areas in DoD. This report provides coverage of the Information Security high-risk area.

Prior Coverage

During the last 5 years, the GAO has issued three reports discussing SSNs. Unrestricted GAO reports can be accessed over the Internet at http://www.gao.gov.

GAO

GAO-02-766, "Greater Awareness and Use of Existing Data are Needed," June 28, 2002

GAO-02-352, "Government Benefits from SSN Use But Could Provide Better Safeguards," May 31, 2002

GAO-99-28, "Government and Commercial Use of the Social Security Number is Widespread," February 16, 1999

Appendix B. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Personnel and Readiness
Assistant Secretary of Defense (Command Control, Communications and Intelligence)
Under Secretary of Defense (Comptroller)/Chief Financial Officer
    Deputy Chief Financial Officer
    Deputy Comptroller (Program/Budget)

Department of the Army

Auditor General, Department of the Army

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force

Other Defense Organizations

Director, Army and Air Force Exchange Service
Director, Defense Manpower Data Center
Director, Defense Security Service

Non-Defense Federal Organization

Office of Management and Budget

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member (cont'd)

House Subcommittee on Technology and Procurement Policy, Committee on Government Reform
House Subcommittee on Ways and Means on Social Security

Department of Defense Manpower Data Center Comments

DEPARTMENT OF DEFENSE

MANPOWER DATA CENTER

REPLY TO DMDC

1600 N. WILSON BLVD., SUITE 400
ARLINGTON, VIRGINIA 22209-2593

DoD CENTER MONTEREY BAY
400 GIGLING ROAD
SEASIDE, CA 93955-6771

April 1, 2002

MEMORANDUM FOR DOD Inspector General for Auditing, ATTN: Mr. Thomas S. Bartoszek

SUBJECT: Audit of Controls Over the Use and Protection of Social Security Numbers Within DoD (D2002AB-0070.00) – Commitment Letter

Mr. Thomas Bartoszek, Mr. Thomas Hilliard, and Ms. Constance Halahan, all members of the DoD Inspector General's Office, were at DMDC from 18 March through 26 March 2002. The purpose of the visit was to look at DMDC's policies and procedures in the Subject area. The following issues were provided by the team to DMDC management.

a. Expand policy and procedure documentation for the agency as required by DoD 5400.11-R 5.4.2.

b. Require outside audit of DMDC's Privacy Program periodically as required by DoD 5400.11-R 5.4.4.

c. Review of the Naval Postgraduate School Computer Center by physical security professionals and cost effective/risk management upgrades installed.

The management of DMDC agrees to:

a. Expand our current DMDC Privacy Release Accounting Policy (PRAS) to include all the steps in the process for a request for individual identifiable data from the time it arrives at DMDC. This policy revision will be completed within one month of this date.

b. Inquiries will be made, within one month of this date, as to what office within DoD can provide periodic review of DMDC's Privacy Program. A date will be set for that review and will be recurring on a biennial basis.

c. The Naval Postgraduate School Computer Center management and the DMDC management will meet with physical security professionals to review the security of the Computer Center. Recommendation will be considered on a cost effective/risk assessment basis. Those suggestions that provide the most security and can be satisfied with dollars available will be installed.

We hope these commitments are responsive to your concerns.

Robert J. Brandewie
Deputy Director

Departments of the Army and Air Force Exchange Service Comments

DEPARTMENTS OF THE ARMY & AIR FORCE
Headquarters Army & Air Force Exchange Service
Dallas, Texas 75266-0202

18 JUN 2002

SUBJECT: Audit of Controls over the Use and Protection of Social Security Numbers within DoD (D2002AB-0070) (Jan 23, 02 letter)

Mr. Thomas S. Bartoszek
Inspector General for Auditing
Department of Defense
400 Army Navy Drive
Arlington, Virginia 22202-4704

1. In compliance with referenced letter, Ms. Lisa Novis and Ms. Mandi Markwart, members of the DoD Inspector General's office, visited and audited the Army and Air Force Exchange Service (AAFES) from March 11 through March 21, 2002, to review policies and procedures over the use and protection of social security numbers (SSNs). The team provided the following suggestions to management:

a. Require uniform Privacy Act statements, confidentiality statements, and requirements for the protection and usage of the information in all contracts that involve the use of Systems of Record information or access.

b. Review the Systems of Records list to ensure it is current and accurate and make any needed additions, deletions, alterations or amendments. For systems such as the Corporate Customer Database, which is covered under another System of Record, document that in the system notice or keep with the system notice.

c. Provide employee training on the DoD Privacy Program, the Privacy Act and the use and protection of SSNs, perhaps incorporate into ethics or security training.

d. Provide Privacy Act oversight and verification of SSN use and protection using the AAFES internal Audit Program to periodically ensure management controls are in place, i.e., audit above suggestions to ensure implementation and compliance.

2. AAFES will:

a. Utilize uniform Privacy Act statements or confidentiality provisions in all contracts where contractors will have access to personal information to include SSNs.

b. Require all Directorates to review applicable systems notices and submit the necessary documentation to cause the notices to be amended as needed.

c. Produce a video for distribution to facilities worldwide concerning the Privacy Act and the use and protection of SSNs.

d. Conduct internal audits concerning actions as stated above.

3. The appropriate use and protection of personal information is an important issue that AAFES is committed to.

CHARLES T. WAX
Major General, USAF
Commander

Defense Security Service Comments

DEFENSE SECURITY SERVICE
1340 BRADDOCK PLACE
ALEXANDRIA, VA 22314-1651

JUN 04 2002

MEMORANDUM FOR INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
ATTN: ROBIN G. McCOY
400 ARMY NAVY DRIVE
ARLINGTON, VA 22202-2885

SUBJECT: Audit of Controls over the Use and Protection of Social Security Numbers Within DoD (D2002AB-0070.00)

This is in response to your May 9, 2002, summary on the review of the Defense Security Service's (DSS) use and protection of Social Security numbers.

Enclosed is the DSS response to your initial findings. Whether dealing with personal information, Privacy Act protected or not, or information which is considered to be FOUO, the DSS takes very seriously any suggestions/advise which helps to protect and preserve the confidentiality of the data we maintain. Accordingly, DSS is very appreciative of your recommendations/findings and the professional manner in which you and Ms. Patrice Cousins conducted this Audit.

If you have any questions with regard to our agency responses, please feel free to contact the undersigned at (703) 325-9450.

LESLIE R. BLAKE
Chief, Office of Freedom of Information and Privacy

Enclosure

1. **None of the contracts with nine private contractors that process privacy act data contained the FAR clause as required by the Privacy Act.**

Response: Although each of the Phase I and Phase II PSI Augmentation Contracts (DynCorp, ManTech, MSM, Omniplex and GBSG) clearly stated Privacy Act requirements within each contract's Statement of Work, we agree that more must be done to ensure that Privacy Act requirements are being met. Accordingly, we have requested that the 11th Contracting Squadron modify each contract to clearly include the Federal Acquisition Regulation (FAR) clauses pertaining to the Privacy Act (clauses 52.224-1 and 52.224-2) in Section I of each contract. We are also looking at adding independent "confidentiality" clauses to future contracts, which would place further restrictions on the contractor as to access to, and use of, the data.

2. **DSS did not adequately monitor the private contracts use of Privacy Act data (including Social Security numbers) to conduct their DSS mission.**

Response: A DSS Contracting Officer Representative (COR) visits each contractor facility each week to review functions associated with the contract. While the principal focus of the visit is to review the quality of the deliverables, the COR also monitors other activities of each contractor. While we feel these measures are steps in the right direction, we concede that we need to put an equal focus on the review of privacy protected information. Accordingly, we will initiate unannounced site visits and include appropriate data protection review as a routine inspection activity. With regard to our credit bureau contracts, the on-site facilities of these three contractors have not been monitored. However, the DSS connection with these contractors systems is purely electronic and involves little or no human interaction. Notwithstanding, DSS will establish a dedicated COR for these contracts (a single COR for all three) and require the COR to communicate regularly with each firm to ensure that no changes have occurred that may impact the protection of the data. We note also that the credit bureaus are required to comply with a number of regulations and laws governing the collection and reporting of the data they maintain, and future DSS contracts with the credit bureaus will be modified to include the FAR clauses. In response to DoDIG's possible concern that a contractor was using an unqualified person to review DSS deliverables, the person in question (if Ms. Monsanto), did, in fact, have a System Access Request (SAR) properly approved on May 23, 2001, which granted her access to the system data as required by DSS policy.

3. **DSS does not have an overarching standard operating procedure that details the mission, functions and responsibilities of the various offices with the agency.** Confusion existed among the various offices concerning the end-to-end process used by DSS to conduct personnel security investigations. (F.SI.33) DSS is in the process of developing a statement of work to submit to the contracting office for solicitation of a private contractor to develop a standard operating procedure. (F.SI.33)

Response: While it is true that DSS currently does not have an UPDATED Standard Operating Procedures (SOP) manual, there is one in existence which is still moderately helpful, though outdated. The SOP, which was last printed in 1993 describes the Personnel Investigations Center (PIC) mission, as well as consolidating all pertinent operational PIC policy and procedures which were in place previous to the implementation of the Case Control Management System (CCMS). Although the process described in the 1993 SOP have now been automated, via CCMS, and procedures for opening, monitoring and closing investigations have changed accordingly, the basic structure of the PSI, as well as the mission of the PIC, has not. This would include the responsibility for the protection of data. To assist in the transition into the world of automation, which is an ongoing process, all PIC employees using the CCMS have been provided with the CCMS handbook. In addition, to the existing SOP and the CCMS Handbook, DSS has the current Personnel Security Investigations Manual, DSS 20-1-M (September 10, 2001), which is used extensively by all DSS employees. This manual provides directions, guidance, and standards for Investigators and Security Specialists regarding the conduct and protection of Personnel Security Investigations. There is one chapter strictly devoted to just the Privacy Act (PA) and disclosure of PA protected information. Because investigative procedures and policies are ever changing, DSS continuously post current policy letters within the DSS Intranet system, which also enables all DSS employees to keep current with agency directives, policy and procedures.

Notwithstanding the above, DSS concurs that it must take all necessary steps to ensure that adequate safeguards are in place to protect and preserve the confidentiality of the date we maintain. A key first step to this process is developing a current SOP which increases the consistency of how data is to be processed, and protected. Consequently, DSS is in the process of obtaining contractual support for the development and publication of a current SOP.

Team Members

The Acquisition Management Directorate, Office of the Assistant Inspector General for Auditing, DoD, prepared this report. Personnel of the Office of the Inspector General, DoD, who contributed to the report are listed below.

Mary L. Ugone
Bruce A. Burton
Thomas S. Bartoszek
Lisa E. Novis
Thomas J. Hilliard
Robin G. McCoy
Thelma E. Jackson
Patrice A. Cousins
Mandi L. Markwart
Constance E. Wojtek
Jennifer L. Jezewski
Jenshel D. Marshall
Jacqueline N. Pugh